

# Notice of Allowability

Application No.

10/718,375

Examiner

Ronald Baum

Applicant(s)

SZOR ET AL.

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/6/2007.
2. ☒ The allowed claim(s) is/are 1-10, 12-26 and 28-33.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

## Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

9,27,07

## DETAILED ACTION

### *Examiner's Statement of Reasons for Allowance*

1. Claims 1-10, 12-26 and 27-33 are allowed over prior art.
2. This action is in reply to applicant's correspondence of 06 August 2007.
3. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.
4. As per claims 1, 24 and 30 generally, prior art of record, Muttik et al, U.S. Patent Application Publication 2003/0023864 A1, fails to teach alone, or in combination, at the time of the invention, the features as discussed and remarked upon in the response of 06 August 2007 to office action of 20 June 2007.

Specifically, (as per claim 1, for example) prior art dealing with the ability to manage malware detection and mitigation, insofar as *generic methods generally*, and technological solutions such as via integrity management techniques such as detection of suspicious or multiple file extensions, more particularly (i.e., file modification that shows the harmless first extension (i.e., .txt, .jpg, etc.), but hides the second extension (i.e., .EXE, .VBS, etc.); Lee, A., et al, 'Back to the Future - Fresh Approaches to Malware Management', EICAR Conf. Proceedings 2002, pp. 76-109, <http://www.aomr.co.uk/papers/lee-harley.pdf>), is generally known per se. Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., the various aspects of stalling a critical OS function call prior to determination of the last, next to last file name extensions and the determination of the multiple extensions to be dangerous, and subsequent generation of notification with possible computer protective actions taken upon such determination), at the *time of the invention*, serving to patently distinguish the invention from said prior art;

“1. A method comprising:

*stalling a file system event,*

*said file system event including a file name;*

*parsing said file name to obtain at least*

*a last file name extension, and*

*a next to last file name extension, when present,*

*of said file name;*

*determining whether said last file name extension is*

*the only file name extension of said file name;*

*upon a determination that said last file name extension is*

*not the only file name extension of said file name,*

*determining whether said last file name extension is*

*a dangerous file name extension; and*

*upon a determination that said last file name extension is*

*a dangerous file name extension,*

*generating a notification.”.*

5. Dependent claims 2-10, 12-23, 25, 26, 28, 29, 31-33 are allowable by virtue of their dependencies.


*Conclusion*

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
9,27,07

Ronald Baum

Patent Examiner

